

## PATENT

## REMARKS

Claims 1-24 are pending in the application. Claims 1-24 have been rejected.

**Claim Rejections under 35 U.S.C. §112**

Claims 1-24 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

The Examiner rejected claim 1 and indicated that the specification does not describe an out-of-band channel, encrypting the first key with the registration key, sending the unencrypted first key on a broadcast channel, encrypting the second key with the first key and sending the second key on an out-of-band channel.

Applicants have amended claim 1 and submit that the claim and the amendments are fully supported by the specification. The Examiner stated that the specification does not describe encrypting the first key with the registration key. Applicant respectfully submits that encrypting the first key with the registration key is disclosed in paragraph 1062: "In the subscription process the CS sends the UIM 308 the value of a common Broadcast Access Key (BAK). The CS sends the MS 300, and specifically UIM 308, the value of BAK encrypted using the RK unique to UIM 308." In addition, the Examiner stated that the specification does not describe encrypting the second key with the first key. Applicants respectfully submit that encrypting the second key with the first key is disclosed in paragraphs 1066 and 1068. "To ensure the efficient distribution of the security information SK, the CS periodically distributes a common Broadcast Access Key (BAK) to each subscriber UIM 308. For each subscriber the CS encrypts BAK using the corresponding RK to obtain a value called BAKI (BAK information). The CS sends the corresponding BAKI to the MS 300 of the subscribed user." (paragraph 1066) "Within each period for updating the BAK, a short-term interval is provided during which SK is distributed on a broadcast channel." (paragraph 1068) Therefore, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Claims 2-10 are allowable as depending directly or indirectly from allowable amended claim 1.

Claim 22 is allowable for the same reasons given above for claim 1.

Attorney Docket No.: 010497  
Customer No.: 23696

**PATENT**

Claims 15-21 were rejected by the Examiner because the specification does not disclose sending a first and second key unencrypted over a channel. Applicants respectfully request that this rejection be withdrawn because claim 15 does not disclose sending a first and second key unencrypted over a channel, either in the previous or current amended versions. Claim 15 discloses that the first key is "encrypted with the registration key" and the second key is "encrypted with the first key". Therefore, Applicants submit that amended claim 15 is allowable.

Claims 16-21 are allowable as depending either directly or indirectly from allowable claim 15.

Claims 15-21 were also rejected by the Examiner stated that the specification does not disclose the combination of a first key, second key, short term key and registration key. Applicants respectfully submit that the above terms are disclosed in the specification. Particular paragraphs have been cited above which indicate that the specification does disclose these terms. Applicants request, therefore, that the rejection of claims 15-21 be withdrawn.

Claims 1-14 and 22-24 were rejected by the Examiner on the basis of the specification not disclosing the combination of limitations comprising encrypting a first key with a registration key, encrypting a second key with a first key, and sending the second key on an out-of-band channel. Applicants have amended the claims to remove the reference to an out-of-band channel. However, Applicants respectfully submit that the limitations encrypting a first key with a registration key, encrypting a second key with a first key, are disclosed within the specification in the paragraphs cited above. Therefore, Applicants submit that claims 1-14 and 22-24 are in condition for allowance.

**Claim Rejections under 35 U.S.C. § 101**

Claim 24 was rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. The Examiner stated that claim 24 recites "a digital signal storage device", and a digital signal does not fall under the statutory classes of invention and therefore the elements of the claim are not tangibly embodied. Applicants have amended claim 24 to recite "a digital data storage device".

Attorney Docket No.: 010497

Customer No.: 23696

## PATENT

**Claim Rejections under 35 U.S.C. § 102(e)**

Claims 15, 16, and 18-21 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,690,795 to Richards (hereinafter "Richards"). Applicants respectfully disagree for the reasons and explanations set forth below.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (Aug. 2001) (*quoting Verdegall Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the . . . claim." *Id.* (*quoting Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1051, 1053 (Fed. Cir. 1987)). In addition, "the reference must be enabling and describe the applicant's invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention." *In re Paulsen*, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994).

Applicants respectfully submit that claims 15, 16, and 18-21 are not anticipated by Richards for the reasons and explanations set forth below.

With respect to amended claim 15 Applicants respectfully submit that Richards does not disclose all the limitations of amended claim 15. In particular, Richards does not disclose "receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel".

Richards discloses an encryption system for restricted-access television systems. A television program is delivered to a customer in the form of a stream of digital data, along a data link, such as a coaxial cable. (Col. 2, lines 41-43). The channels typically have sufficient bandwidth to carry multiple television programs. (Col. 2, lines 45-47). Time multiplexing is used to transmit the channel in the form of digital data packets. (Col. 2, lines 52-56). Each customer has a set top box which includes a decoder to decode and process the packets. (Col. 2, lines 63-65). The data packets are distributed in parallel to all customers. All customers receive all the packets for all programs broadcast. However, customers are only granted access to the specific

Attorney Docket No.: 010497

Customer No.: 23696

**PATENT**

programs provided in their subscriptions. (Col. 3, lines 5-11). The Access Control system distributes decryption keys to customers. The distribution is typically accomplished by sending each customer the decryption keys in encrypted form. (Col. 4, lines 55-59). Each customer's set top box is assigned a unique key. The decryption keys are encrypted using the customer's set top box key. This results in each customer obtaining only the decryption keys for the programs intended for that customer. (Col. 4, lines 59-62). The key, SK, is itself encrypted using another key, PK. Each customer receives two data words. The key SK is encrypted using PK, a program key. PK is encrypted using the unique key of the customer's set top box. (Col. 9, lines 12-18). Both keys, SK and PK are delivered by an out of band channel. (Col. 9, lines 21-22). Key SK is encrypted using PK as a key and is decrypted at the customer using actual PK to produce actual SK and thus produce the content. (Col. 9, lines 25-31) While Richards discloses updating the encryption keys, no specific method for accomplishing this updating is described. Therefore, Richards does not disclose "receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel". Applicants respectfully submit that amended claim 15 is not anticipated by Richards.

Claims 16 and 18-21 are allowable as depending either directly or indirectly from allowable amended claim 15 and are allowable for the same reasons given above for claim 15.

**Claim Rejections under 35 U.S.C. § 103**

Claim 17 was rejected as being unpatentable over U.S. Patent 6,690,795 to Richards as applied to claim 15 in further view of U.S. Patent 6,073,122 to Wool (hereinafter "Wool"). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure." In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Attorney Docket No.: 010497

Customer No.: 23696

**PATENT**

Applicants respectfully submit that a prima facie case of obviousness has not been established regarding claim 17 because the prior art cited does not teach or suggest all the claim limitations.

Wool teaches a system for restricting access to transmitted programming content. The encryption key is transmitted to the customer with the encrypted programming content. A set-top terminal or similar mechanism restricts access to the transmitted multimedia information using stored decryption keys. (Abstract) The set-top terminal preferably receives one or more package keys that are periodically sent by the service provider. Each key corresponds to a package of programs that the customer is entitled to for a given period. (Abstract). Each program is encrypted by the head-end server before transmission using a program key, unique to the program. (Abstract) The memory in the set-top terminal securely stores the decryption keys. (Col. 1, lines 44-46)

Neither Richards nor Wool teaches or suggests the limitation "receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel". Applicants respectfully submit that claim 17 is allowable as the combination of Richards and Wool does not result in Applicants disclosure and request that the rejection of claim 17 be withdrawn.

## PATENT

## REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: August 23, 2005

By: Roberta A. Young  
Roberta A. Young, Reg. No. 53,813  
(858) 658-5803

QUALCOMM Incorporated  
5775 Morehouse Drive  
San Diego, California 92121  
Telephone: (858) 658-5787  
Facsimile: (858) 658-2502

Attorney Docket No.: 010497  
Customer No.: 23696

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**